

A subset of  $\mathbb{Z}^n$  whose non-computability leads  
to the existence of a Diophantine equation  
whose solvability is logically undecidable

Apoloniusz Tyszk

**Abstract.** For  $K \subseteq \mathbb{C}$ , let  $B_n(K) = \{(x_1, \dots, x_n) \in K^n : \text{for each } y_1, \dots, y_n \in K \text{ the conjunction}$

$$\begin{aligned} & \left( \forall i \in \{1, \dots, n\} (x_i = 1 \implies y_i = 1) \right) \wedge \\ & \left( \forall i, j, k \in \{1, \dots, n\} (x_i + x_j = x_k \implies y_i + y_j = y_k) \right) \wedge \\ & \left( \forall i, j, k \in \{1, \dots, n\} (x_i \cdot x_j = x_k \implies y_i \cdot y_j = y_k) \right) \end{aligned}$$

implies that  $x_1 = y_1\}$ . We claim that there is an algorithm that for every computable function  $f : \mathbb{N} \rightarrow \mathbb{N}$  returns a positive integer  $m(f)$ , for which a second algorithm accepts on the input  $f$  and any integer  $n \geq m(f)$ , and returns a tuple  $(x_1, \dots, x_n) \in B_n(\mathbb{Z})$  with  $x_1 = f(n)$ . We compute an integer tuple  $(x_1, \dots, x_{20})$  for which the statement  $(x_1, \dots, x_{20}) \in B_{20}(\mathbb{Z})$  is equivalent to an open Diophantine problem. We prove that if the set  $B_n(\mathbb{Z})$  ( $B_n(\mathbb{N})$ ,  $B_n(\mathbb{N} \setminus \{0\})$ ) is not computable for some  $n$ , then there exists a Diophantine equation whose solvability in integers (non-negative integers, positive integers) is logically undecidable.

**Key words and phrases:** Hilbert's Tenth Problem, logically undecidable Diophantine equation.

**2010 Mathematics Subject Classification:** 03D20, 11U05.

For  $K \subseteq \mathbb{C}$ , let  $B_n(K) = \{(x_1, \dots, x_n) \in K^n : \text{for each } y_1, \dots, y_n \in K \text{ the conjunction}$

$$\begin{aligned} & \left( \forall i \in \{1, \dots, n\} (x_i = 1 \implies y_i = 1) \right) \wedge \\ & \left( \forall i, j, k \in \{1, \dots, n\} (x_i + x_j = x_k \implies y_i + y_j = y_k) \right) \wedge \\ & \left( \forall i, j, k \in \{1, \dots, n\} (x_i \cdot x_j = x_k \implies y_i \cdot y_j = y_k) \right) \end{aligned}$$

implies that  $x_1 = y_1\}$ .

Each of the following two statements

$$\begin{aligned} & (164, 165, 164 \cdot 165, (164 \cdot 165)^2, \\ & 132, 133, 132 \cdot 133, (132 \cdot 133)^2, \\ & 143, 144, 143 \cdot 144, (143 \cdot 144)^2, 1) \in B_{13}(\mathbb{N} \setminus \{0\}) \end{aligned}$$

and

$$\begin{aligned} & (164, 165, 164 \cdot 165, (164 \cdot 165)^2, \\ & 131, 132, 133, 132 \cdot 133, (132 \cdot 133)^2, \\ & 142, 143, 144, 143 \cdot 144, (143 \cdot 144)^2, 1) \in B_{15}(\mathbb{N}) \end{aligned}$$

equivalently expresses that in the domain of positive integers only the triples  $(132, 143, 164)$  and  $(143, 132, 164)$  solve the equation

$$x^2(x+1)^2 + y^2(y+1)^2 = z^2(z+1)^2$$

The last claim is still not proved, see [2, p. 53].

The following Lemma is a special case of the result presented in [4, p. 3].

**Lemma** ([6, p. 177, Lemma 2.1]). *For each non-zero integer  $x$  there exist integers  $a, b$  such that  $ax = (2b - 1)(3b - 1)$ .*

*Proof.* Write  $x$  as  $(2y - 1) \cdot 2^m$ , where  $y \in \mathbb{Z}$  and  $m \in \mathbb{Z} \cap [0, \infty)$ . Obviously,  $\frac{2^{2m+1} + 1}{3} \in \mathbb{Z}$ . By Chinese Remainder Theorem, we can find an integer  $b$  such that  $b \equiv y \pmod{2y - 1}$  and  $b \equiv \frac{2^{2m+1} + 1}{3} \pmod{2^m}$ . Thus,  $\frac{2b - 1}{2y - 1} \in \mathbb{Z}$  and  $\frac{3b - 1}{2^m} \in \mathbb{Z}$ . Hence

$$\frac{(2b - 1)(3b - 1)}{x} = \frac{2b - 1}{2y - 1} \cdot \frac{3b - 1}{2^m} \in \mathbb{Z}$$

□

Let  $b = 200526827$ . Then,

$$667378345 \cdot (132 \cdot 133 \cdot 143 \cdot 144) = (2b - 1)(3b - 1)$$

**Theorem 1.** *The statement*

$$(164 \cdot 165, (164 \cdot 165)^2, 164, 165,$$

$$132, 133, 132 \cdot 133, (132 \cdot 133)^2,$$

$$143, 144, 143 \cdot 144, (143 \cdot 144)^2, 132 \cdot 133 \cdot 143 \cdot 144,$$

$$b, 2b, 2b - 1, 3b - 1, (2b - 1)(3b - 1), \frac{(2b - 1)(3b - 1)}{132 \cdot 133 \cdot 143 \cdot 144}, 1) \in B_{20}(\mathbb{Z})$$

*equivalently expresses that in the integer domain only the triples  $(x, y, z) \in$*

$$\left( \{-133, 132\} \times \{-144, 143\} \times \{-165, 164\} \right) \cup \left( \{-144, 143\} \times \{-133, 132\} \times \{-165, 164\} \right)$$

*solve the system*

$$\begin{cases} x^2(x + 1)^2 + y^2(y + 1)^2 &= z^2(z + 1)^2 \\ x(x + 1)y(y + 1) &\neq 0 \end{cases}$$

*Proof.* The following *MuPAD* code

```

y:=(132*133*143*144/64+1)/2:
z:=(2^13+1)/3:
print('b='):
b:=numlib::ichrem([y,z],[2*y-1,64]);
print('(2b-1)(3b-1)/(132*133*143*144)='):
(2*b-1)*(3*b-1)/(132*133*143*144);
A:=[164*165,(164*165)^2,164,165,
132,133,132*133,(132*133)^2,
143,144,143*144,(143*144)^2,132*133*143*144,
b,2*b,2*b-1,3*b-1,(2*b-1)*(3*b-1),
(2*b-1)*(3*b-1)/(132*133*143*144),1]:
print('the triples [i,j,k] with i<=j and A[i]+A[j]=A[k]'):
for i from 1 to 20 do
for j from i to 20 do
for k from 1 to 20 do
if A[i]+A[j]=A[k] then print([i,j,k]) end_if:
end_for:
end_for:
end_for:
print('the triples [i,j,k] with i<=j<20 and A[i]*A[j]=A[k]'):
for i from 1 to 19 do
for j from i to 19 do
for k from 1 to 20 do
if A[i]*A[j]=A[k] then print([i,j,k]) end_if:
end_for:
end_for:
end_for:

```

returns the output

```

        'b='
        200526827
        '(2b-1)(3b-1)/(132*133*143*144)='
        667378345
        'the triples [i,j,k] with i<=j and A[i]+A[j]=A[k] '
            [3, 20, 4]
            [5, 20, 6]
            [8, 12, 2]
            [9, 20, 10]
            [14, 14, 15]
            [14, 16, 17]
            [16, 20, 15]
        'the triples [i,j,k] with i<=j<20 and A[i]*A[j]=A[k] '
            [1, 1, 2]
            [3, 4, 1]
            [5, 6, 7]
            [7, 7, 8]
            [7, 11, 13]
            [9, 10, 11]
            [11, 11, 12]
            [13, 19, 18]
            [16, 17, 18]

```

At the start, the code computes the integer  $b$  by applying the algorithm presented in the proof of the Lemma. Next, the code computes  $\frac{(2b-1)(3b-1)}{132 \cdot 133 \cdot 143 \cdot 144}$ . The triples displayed on the output justify the equivalence.  $\square$

**Theorem 2.** *The statement*

$$\begin{aligned} & (328, 330, 328 \cdot 330, (328 \cdot 330)^2, \\ & 264, 266, 264 \cdot 266, (264 \cdot 266)^2, \\ & 286, 288, 286 \cdot 288, (286 \cdot 288)^2, \\ & 250, 16, 4, 2, 1) \in B_{17}(\mathbb{N} \setminus \{0\}) \end{aligned}$$

*equivalently expresses that in the domain of positive integers only the triples (250, 286, 328) and (272, 264, 328) solve the equation*

$$(x + 14)^2(x + 16)^2 + y^2(y + 2)^2 = z^2(z + 2)^2$$

*The last claim about a possible solutions to the above equation can be equivalently formulated thus: in the domain of integers greater than 1, only the triples*

$$(10, 13, 14), (13, 10, 14), (265, 287, 329), (287, 265, 329)$$

*solve the equation*

$$(x^2 - 1)^2 + (y^2 - 1)^2 = (z^2 - 1)^2$$

*For the last equation, no other solutions are known, see [3, p. 68].*

*Proof.* The following MuPAD code

```
A:=[328,330,328*330,(328*330)^2,
264,266,264*266,(264*266)^2,
286,288,286*288,(286*288)^2,
250,16,4,2,1]:
print('the triples [i,j,k] with i=<j and A[i]+A[j]=A[k]'):
for i from 1 to 17 do
for j from i to 17 do
for k from 1 to 17 do
```

```

if A[i]+A[j]=A[k] then print([i,j,k]) end_if:
end_for:
end_for:
end_for:
print('the triples [i,j,k] with i=<j<17 and A[i]*A[j]=A[k]'):
for i from 1 to 16 do
for j from i to 16 do
for k from 1 to 17 do
if A[i]*A[j]=A[k] then print([i,j,k]) end_if:
end_for:
end_for:
end_for:

```

returns the output

```

'the triples [i,j,k] with i=<j and A[i]+A[j]=A[k]'
    [1, 16, 2]
    [5, 16, 6]
    [8, 12, 4]
    [9, 16, 10]
    [13, 14, 6]
    [16, 16, 15]
    [17, 17, 16]
'the triples [i,j,k] with i=<j<17 and A[i]*A[j]=A[k]'
    [1, 2, 3]
    [3, 3, 4]
    [5, 6, 7]
    [7, 7, 8]
    [9, 10, 11]
    [11, 11, 12]

```

[15, 15, 14]

[16, 16, 15]

The triples displayed on the output justify the first equivalence. The second equivalence is obvious.  $\square$

The sets  $B_n(\mathbb{Z})$  contain very non-trivial integer tuples as it follows from the next theorem.

**Theorem 3.** *There is an algorithm that for every computable function  $f : \mathbb{N} \rightarrow \mathbb{N}$  returns a positive integer  $m(f)$ , for which a second algorithm accepts on the input  $f$  and any integer  $n \geq m(f)$ , and returns a tuple  $(x_1, \dots, x_n) \in B_n(\mathbb{Z})$  with  $x_1 = f(n)$ .*

*Proof.* The author proved in [5] that there is an algorithm that for every computable function  $f : \mathbb{N} \rightarrow \mathbb{N}$  returns a positive integer  $m(f)$ , for which a second algorithm accepts on the input  $f$  and any integer  $n \geq m(f)$ , and returns a system

$$S \subseteq \{x_i = 1, x_i + x_j = x_k, x_i \cdot x_j = x_k : i, j, k \in \{1, \dots, n\}\}$$

such that  $S$  is consistent over the integers and each integer tuple  $(x_1, \dots, x_n)$  that solves  $S$  satisfies  $x_1 = f(n)$ . Let  $\leq_n$  denote the order on  $\mathbb{Z}^n$  which ranks the tuples  $(x_1, \dots, x_n)$  first according to  $\max(|x_1|, \dots, |x_n|)$  and then lexicographically. The ordered set  $(\mathbb{Z}^n, \leq_n)$  is isomorphic to  $(\mathbb{N}, \leq)$ . To find an integer tuple  $(x_1, \dots, x_n)$ , we solve the system  $S$  by performing the brute-force search in the order  $\leq_n$ .  $\square$

The presented results lead to the following Conjecture.

**Conjecture.** *For each sufficiently large  $n$ , the sets  $B_n(\mathbb{Z})$ ,  $B_n(\mathbb{N})$  and  $B_n(\mathbb{N} \setminus \{0\})$  are not computable.*

The conclusion of the following Theorem 4 is unconditionally true and well-known as the corollary of the negative solution to Hilbert's Tenth Problem, see [1, p. 231].



**Theorem 4.** *If the set  $B_n(\mathbb{Z})$  is not computable for some  $n$ , then there exists a Diophantine equation whose solvability in integers is logically undecidable.*

*Proof.* By the Lemma, for each integers  $a_1, y_1$  the statement  $a_1 \neq y_1$  is equivalent to

$$\exists a, b \in \mathbb{Z} \ a(a_1 - y_1) - (2b - 1)(3b - 1) = 0$$

To an integer tuple  $(a_1, \dots, a_n)$  we assign the equation

$$D_{(a_1, \dots, a_n)}(a, b, y_1, \dots, y_n) = (a(a_1 - y_1) - (2b - 1)(3b - 1))^2 + \sum_{\substack{i \in \{1, \dots, n\} \\ a_i = 1}} (y_i - 1)^2 + \sum_{\substack{(i, j, k) \in \{1, \dots, n\}^3 \\ a_i + a_j = a_k}} (y_i + y_j - y_k)^2 + \sum_{\substack{(i, j, k) \in \{1, \dots, n\}^3 \\ a_i \cdot a_j = a_k}} (y_i \cdot y_j - y_k)^2 = 0$$

For each integers  $a_1, \dots, a_n$ , the tuple  $(a_1, \dots, a_n)$  does not belong to  $B_n(\mathbb{Z})$  if and only if the equation  $D_{(a_1, \dots, a_n)}(a, b, y_1, \dots, y_n) = 0$  has a solution in integers  $a, b, y_1, \dots, y_n$ . We prove that there exists an integer tuple  $(a_1, \dots, a_n)$  for which the solvability of the equation  $D_{(a_1, \dots, a_n)}(a, b, y_1, \dots, y_n) = 0$  in integers  $a, b, y_1, \dots, y_n$  is logically undecidable. Suppose, on the contrary, that for each integers  $a_1, \dots, a_n$  the solvability of the equation  $D_{(a_1, \dots, a_n)}(a, b, y_1, \dots, y_n) = 0$  can be either proved or disproved. This would yield the following algorithm for deciding whether an integer tuple  $(a_1, \dots, a_n)$  belongs to  $B_n(\mathbb{Z})$ : examine all proofs (in order of length) until for the equation  $D_{(a_1, \dots, a_n)}(a, b, y_1, \dots, y_n) = 0$  a proof that resolves the solvability question one way or the other is found.  $\square$

Similarly, but simpler, if the set  $B_n(\mathbb{N})$  ( $B_n(\mathbb{N} \setminus \{0\})$ ) is not computable for some  $n$ , then there exists a Diophantine equation whose solvability in non-negative integers (positive integers) is logically undecidable.

## References

- [1] V. Klee and S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, Mathematical Association of America, Washington, DC, 1991.
- [2] W. Sierpiński, *Elementary theory of numbers*, 2nd ed. (ed. A. Schinzel), PWN (Polish Scientific Publishers) and North-Holland, Warsaw-Amsterdam, 1987.
- [3] W. Sierpiński, *O rozwiązywaniu równań w liczbach całkowitych* (in Polish) [*On solving equations in integers*], 2nd ed. (ed. J. Browkin and A. Schinzel), PWN (Polish Scientific Publishers), Warsaw, 2009.
- [4] Th. Skolem, *Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist*, Avh. Norske Vid. Akad. Oslo. I. (1942), no. 4.
- [5] A. Tyszk, *A new characterization of computable functions*, <http://arxiv.org/abs/1011.4103>.
- [6] A. Tyszk, *Two conjectures on the arithmetic in  $\mathbb{R}$  and  $\mathbb{C}$* , MLQ Math. Log. Q. 56 (2010), no. 2, 175–184.

Apoloniusz Tyszk  
Technical Faculty  
Hugo Kołłątaj University  
Balicka 116B, 30-149 Kraków, Poland  
E-mail address: rttyszk@cyf-kr.edu.pl